6. What is claimed is:

1. A tamper-resistant modular multiplication method for calculating a modular multiplication, A*B*R^(-1) mod N, which appears during crypto-processing, utilizing an information processing device comprising the steps of:

(1) calculating S_1 = A*B*R^(-1) mod N;

(2) in place of the step (1), calculating S_2 = {sN + A*(-1)^f}*{tN + B*(-1)^g}R^(-1) mod N, (among s, t, f, g, at least one is an integer excepting 0, and f, g are both 0 or 1);

(3) properly selecting the step (1) or (2);

(4) properly repeating the above-mentioned steps (1), (2), (3), wherein finally when the step (1) is selected, for a calculation result S_1, T_1 = S_1*R^(-1) mod N is calculated to output T_1, and when the step (2) is selected, for a calculation result S_2, T_2 = S_2*R^(-1) mod N is calculated to output N − T_2; and

(5) using T_1 and N − T_2 as a calculation result of a modular multiplication, A*B*R^(-1) mod N.

2. A tamper-resistant modular multiplication method of claim 1, wherein said properly selecting in the step (3) means to select either one using random numbers.

3. A tamper-resistant modular multiplication method of claim 1, wherein said (s, t, f, g) are (0, 1, 0, 1).

4. A tamper-resistant modular multiplication method of claim 1, wherein said (s, t, f, g) are (1, 0, 1, 0).

5. A tamper-resistant modular multiplication method for calculating a modular multiplication, A*B mod p (p is a prime), which appears during crypto-processing, utilizing an information processing device, comprising the steps of:

(1) calculating S = A*B mod p;

(2) in place of the step (1), calculating S = {Sp + A*(-1)^F}*{Tp + B*(-1)^G} mod p (among s, t, f, g, at least one is an integer excepting 0, f and g are both 0 or 1, and f + g is an even number);

(3) properly selecting the step (1) or (2);

(4) using the calculation result S which is selected from said step (1) or (2) as a calculation result of a modular multiplication, A*B mod p.

6. A tamper-resistant modular multiplication method of claim 5, wherein said (s, t, f, g) are (1, 1, 1, 1).

7. A tamper-resistant modular multiplication method of claim 5, wherein the value of f + g in said step (2) is an odd number, and

wherein said method further comprising in place of said step (4):

(4) a step wherein when said step (1) is selected

the calculation result S is adopted as it is, and when said step (2) is selected, $p - S$ is adopted as a calculation result in place of S; and

(5) a step for adopting said S and $p - S$ as a calculation result of a modular multiplication operation, $A*B \bmod p$, for crypto-processing.

8. A tamper-resistant modular multiplication method of claim 7, wherein said (s, t, f, g) are $(0, 1, 0, 1)$.

9. A tamper-resistant modular multiplication method for calculating a modular multiplication, $A(x)*B(x) \bmod \Phi(x)$, which appears during crypto-processing, utilizing an information processing device, wherein $\Phi(x)$ is an irreducible polynomial of x and the operation of coefficients of $A(x)*B(x)$ is performed for modulus of a prime p which is 3 or more), comprising the steps of:

(1) calculating $S(x) = A(x)*B(x) \bmod \Phi(x)$;

(2) in place of the step (1), calculating $S(x) = \{s\Phi(x) + A(x)*(-1)^f\}*\{t\Phi(x) + B(x)*(-1)^g\} \bmod \Phi(x)$ (among s, t, f, g, at least one is an integer excepting 0, f and g are both 0 or 1, and $f + g$ is an even number);

(3) properly selecting the step (1) or (2);

(4) using the calculation result $S(x)$ which is selected from said step (1) and (2) as a calculation result of a modular multiplication, $A(x)*B(x) \bmod \Phi(x)$, for crypto-processing.

10. A tamper-resistant modular multiplication method of claim 9, wherein said (s, t, f, g) are (1, 1, 1, 1).

11. A tamper-resistant modular multiplication method of claim 9, wherein the value of f + g in the step (2) is an odd number, and wherein said method further comprises in place of said step (4):

(4) a step wherein when the step (1) is selected the calculation result S(x) is adopted as it is, and when said step (2) is selected, $\Phi(x) - S(x)$ is adopted as a result of calculation result in place of S(x); and

(5) a step for adopting said S(x) and $\Phi(x) - S(x)$ as a calculation result of a modular multiplication operation, A(x)*B(x) mod $\Phi(x)$, for crypto-processing.

12. A tamper-resistant modulus multiplication method of claim 11, wherein said (s, t, f, g) are (0, 1, 0, 1).

13. A tamper-resistant modular multiplication method of claim 9, wherein said the operation of the coefficients of A(x)*B(x) is performed for modulus of a prime 2 and (f, g) in said step (2) are (0, 0).